REMARKS

The present amendment is submitted in response to the Office Action mailed April 4, 2008. Claims 1-13 remain in this application. In view of the amendments above and the remarks to follow, reconsideration and allowance of this application are respectfully requested.

Interview Summary

Applicant appreciates the courtesy granted to Applicant's attorney, Michael A. Scaturro (Reg. No. 51,356), during a telephonic interview conducted on Tuesday, May 13, 2008. During the interview, Applicant's attorney provided a general description of the reproducing apparatus and corresponding reproducing method for reproducing content stored in encrypted form on a record carrier. In providing the general description, Applicant's attorney referred to a visual aid (flowchart diagram) and a copy of claim 1 with certain portions highlighted. The flowchart diagram diagrammatically tracked the elements of claim 1.

During the interview, Applicant's attorney pointed out that the invention provides a higher security against hacking because the record carrier stores a carrier region code (RCC) in which region the content shall be allowed to be reproduced and an encrypted region key (RK) for decrypting the content. Higher security is provided via a multi-tiered protection scheme in which region codes are first checked, and only upon satisfying the region code test will the encrypted region key (RK) be decrypted for use in

decrypting encrypted content. The parameters, RCC and RK, each stored on the record

carrier, are used together with other parameters stored in the reproducing apparatus, RCD

and DK, to provide higher security against hacking.

The Examiner appreciated the uniqueness of the multi-tiered protection scheme

and requested that the Applicant's response to the outstanding Office Action indicate

where support may be found in the specification for the parameters RCC and RK.

Applicant's attorney agreed to provide such support in the response.

Next, Applicant's attorney and the Examiner reviewed Bednarak to determine

whether this reference teaches the parameters RCC and RK, as used in the context of the

specification and claims. It was concluded that Bednarak teach storing an encrypted

region key (RK) on a record carrier and decrypting the region key (RK) upon satisfying a

region code check (RCC=RCD).

Lastly, the Examiner requested that the Applicant provide support for the

recitation "record carrier", as used in the claim, and in particular with reference to claim

12. Applicant respectfully refers the Examiner to paragraph 34 of the specification which

recites,

[0034] A block diagram of a reproducing apparatus 1 and a **record carrier 2** according to the present invention are shown in FIG. 1. **The record carrier, for instance a CD, DVD or BD disc,** comprises a carrier region code RCC (Region Code Carrier) stored in a region code memory 21, at least one encrypted region key RK stored in a region key memory 22 and encrypted content, for instance audio data, video data, software or any other kind of information, are stored in a content memory 23. In order to reproduce the encrypted content a suitable reproducing apparatus 1, for instance a suitable DVD drive, is to be used. In order to control which record carriers 2 can be reproduced in which regions appropriate means are provided on the record carrier 2 as well as in the reproducing apparatus 1 which work together in the way explained in the following.

The Invention

8

It is instructive to briefly review the invention which implements region codes in a very secure way. According to the invention, a record carrier having (storing) a wrong carrier region code (RCC) will not play in a reproducing apparatus (player) in the same way in which a revoked player can not play a new record carrier. Reproducing devices in different regions store a different device key (DK). Record carriers for a particular region will not include a carrier region code (RCC), for reproducing apparatus from other regions.

According to a method of operation, the region code (RCC) is retrieved from the record carrier and checked first, i.e. it is checked if the carrier region code (RCC) stored on the record carrier matches a device region code (DK) stored in the reproducing apparatus. Only if this check gives a positive result, will a region key (RK), also stored on the record carrier be decrypted using a device key (DK), stored in the reproducing apparatus. The encrypted region key (RK) is finally used to decrypt encrypted content read from the record carrier. With this solution there will be no easy hack to allow playing of record carriers having region codes not matching the device region code. Further, making the player region code free would be equivalent to breaking a copy protection system.

In compliance with the Examiner's request for references from the specification identifying usage of the region code (RCC) and region key (RK), Applicant respectfully submits that paragraph 5 of the specification discloses the elements of the apparatus of

the invention including specific references to the carrier region code (RCC) and the

region key (RK).

[0005] This object is achieved according to the present invention by a reproducing apparatus for reproducing content stored in encrypted form on a record carrier, said record carrier further storing **a carrier region code** indicating in which region said content shall be allowed to be reproduced and **an encrypted region key** for decrypting said content,...... said reproducing apparatus comprising: [0006] a region code storage means for storing a device region code, [0007] a device key storage means for storing a device key, said device key being different for all regions, [0008] a carrier region code reading means for reading said carrier region code from said record carrier, [0009] a region code check unit for checking if said **carrier region code** matches said device region code, [0010] a region key reading means for reading said **encrypted region key** from said record carrier, [0011] a region key decryption means for decrypting said **encrypted region key** using said device key in case said **carrier region code** matches said device region code, [0012] a content reading means for reading said decrypted content from said record carrier, [0013] a content decryption means for decrypting said encrypted content using said **decrypted region key** and [0014] output means for outputting said decrypted content. [Emphasis Added]

Paragraph 16 of the Specification teaches describes the method of the invention as

it relates to the use of the carrier region code (RCC) and the region key (RK).

[0016] one main aspect of the proposed invention is that devices in different regions store a different device key. Then, record carriers for a particular region will not include entries, in particular **a carrier region code**, for devices from other regions. According to the present invention, the **region code** is checked first, i.e. it is checked if the **carrier region code** stored on the record carrier matches a device region code stored in the

reproducing apparatus. Only if this check gives a positive result, **a region key** stored also on the record carrier is decrypted using the device key, which **encrypted region key** is finally used to decrypt encrypted content read from the record carrier. With this solution there will be no easy hack to allow playing of record carriers having region codes not matching the device region code. Further, making the player region code free would be equivalent to breaking a copy protection system. [Emphasis Added].

Substantive Rejections

Reference is now made to the substantive rejections of the outstanding Office Action.

35 U.S.C. §103(a)

Claims 1-3 and 9-13 were rejected under 35 U.S.C. §102(b) as being unpatentable over U.S. Patent 6,289,455 – Kocher et al, – hereinafter Kocher and further in view of U.S. Patent 6,009,116 – Bednarak et al. – hereinafter Bednarak. Regarding claim 1, the Examiner asserts that Kocher and Bednarak disclose a reproducing apparatus for reproducing content stored in encrypted form on a record carrier (2), the record carrier further storing a carrier region code (RCC) indicating in which region said content shall be allowed to be reproduced and an encrypted region key (RK) for decrypting said content. The Examiner further asserts, with regard to claim 1 the following:

(1) **Bednarak** discloses: *a region code storage means for storing a device region code (RCD) for use by a region code check unit,*

(2) **Kocher** discloses, *a device storage key means for storing a device key (DK), said device key (DK) being different for all regions,*

(3) **Bednarak** discloses, *a carrier region code reading means for reading said carrier region code (RCC) from said record carrier for use by said region code check unit,*

(4) **Bednarak** discloses: *said region code check unit for checking if said carrier region code (RCC) matches said device region code (RCD) to determine if said record carrier is allowed to be reproduced by said reproducing apparatus,*

(5) **Bednarak** discloses: *a region key reading means for reading said encrypted region key (RK) from said record carrier upon receiving an indication of a match between said device region code (RCD) and said carrier region code (RCC) from said region code check unit.*

(6) **Kocher** discloses: *a region key decryption means for decrypting said region key (RK) using said device key (DK) in case said carrier region code (RCC) matches said device region code (RCD).*

(7) **Kocher** discloses: *a content reading means for reading said encrypted content from said record carrier.* It is respectfully submitted that Kocher does not disclose *a content reading means for reading said encrypted content from said record carrier.*

(8) **Kocher** discloses: *a content decryption means for decrypting said encrypted content using said decrypted region key and output means for outputting said decrypted content.*

It is respectfully submitted that the rejected claims are not unpatentable over Bednarak and Kocher, in any reasonable combination, for at least the following reasons.

Element 5 Not Disclosed by Bednarak

It is respectfully submitted that Bednarak does not disclose: a region key reading means for reading said encrypted region key (RK) from said record carrier upon receiving an indication of a match between said device region code (RCD) and said carrier region code (RCC) from said region code check unit (Element 5 of claim 1 above).

Element 5 performs the action of reading an encrypted region key (RK) from the record carrier whenever an indication of a match between RCC and RD is received... It is necessary to read the encrypted region key (RK) from the record carrier, by the reproducing device to facilitate the decryption of encrypted content on the record carrier. Specifically, encrypted content is retrieved from the record carrier and decrypted using the decrypted region key (RK). Decrypting the region key is taught at element (6).

The Examiner cites Bednarak at col. 20, lines 27-50 for allegedly teaching that Bednarak teaches element 5.

Bednarak discloses at col. 20 that the Region Index is downloaded to each set-top box so that a calculation device or software may compare the downloaded region index with a sensed GPS.

Col. 20, lines 27-50 of Bednarak recites:

> ....The Region Index as input to region comparer 478 is a modified version of the Region Index as determined in method one where it was provided directly from the satellite to each Set-Top box separately. The modification is shown in FIG. 12. The Region Index provided by the Service Provider for each particular Set-Top box is 482 in FIG. 12. Gate 484 serves to pass the Region Index 482 under the condition that the box is actually located in the Region X whose coordinates set is in 486 and whose Index number is 482. Calculation device or software 488 compares the sensed GPS 490 with the coordinate set(s) 486 and outputs a "yes" or enable when the GPS shows the box is in the proper region. is the process which performs the necessary calculations to determine whether the GPS determination performed in 320 is inside Region X.

It is respectfully submitted that col. 20, lines 27-50 of Bednarak does not teach element 5. Instead, col. 20, lines 27-50 of Bednarak teaches whether the actual location of the set-top box (as determined by the sensed GPS) matches a downloaded region index to make a determination regarding whether the set-top box is located in a region authorized to receive the signal.

The Examiner also cites Bednarak at col. 22, lines 51-58 in support of the assertion that Bednarak allegedly teaches element 5.

It is respectfully submitted that col. 22, lines 51-58 of Bednarak does not disclose element 5. Rather, col. 22, lines 51-58 of Bednarak discloses a process for determining whether the GPS coordinates are applicable to a particular local region. This is analogous to determining whether the region carrier code (RCC) is applicable to a device region code (RCD).

It is therefore respectfully submitted that Bednarak does not disclose or suggest element 5. Instead, Bednarak teaches comparing a GPS signal with a Region Index to determine whether the set-top box is physically located in an allowable region to receive the signal.

It is further submitted that Bednarak only discusses encryption in the context of various inputs to system 20 and to the GPS signal and not in the context of decrypting a region key (RK) as taught in element 5.

For example, Bednarak teaches at Col. 8, lines 45 – 60 that various inputs to system 20 are output in encrypted form.

> System 20 also receives program data messages 22 and user authorization data messages 24 supplied by sources (not shown) in a known fashion. Central conditional access system 20 supplies combined data messages 26 (**the various inputs to system 20 output in encrypted form**)

As a further example, Bednarak teaches encryption of a GPS signal at Col. 14, lines 18 – 25:

> In FIG. 5 the dashed line, 340, shows the elements which are co-located inside of the sealed container. The signals which are visible passing into and out of the sealed container are as follows. First, the **encrypted GPS** and conditional

access data 332 from the descrambler and demultiplexor 380 pass into container
340.

Based on the arguments presented above, it is therefore respectfully submitted
that Bednarak does not disclose or suggest element 5 above as alleged in the outstanding
Office Action.

Element 6 Not Disclosed by Kocher

It is respectfully submitted that Kocher does not disclose or suggest a reproducing
apparatus comprising a region key decryption means for **decrypting said region key
(RK) using said device key (DK)** in case said carrier region code (RCC) matches said
device region code (RCD), as asserted in the outstanding Office Action (Element 6 of
claim 1 above).

In accordance with the method of the invention, once the encrypted region key
(RK) is retrieved from the record carrier it must be then be **decrypted** using an
appropriate device key (DK) stored in the reproducing apparatus. The decrypted region
key (RK) is then used by a content decryption means of the reproducing apparatus for
decryption of encrypted content read from the record carrier by content reading means.

The Examiner asserts that element (6) is allegedly taught in Kocher at col. 4,
lines 14-34, col. 7, lines 55-60, col. 8, lines 18-28 & 52-55, col. 9, lines 37-59 and at col.
11, lines 33-65.

Kocher teaches at col. 4, lines 14-24 that software stored in a ROM or EEPROM
manages protocols and cryptographic keys involved in decrypting content. This
process may be assisted by a cryptographic processor. It is submitted managing protocols
and cryptographic keys is different from teaching decrypting said region key (RK) using

15

said device key (DK) in case said carrier region code (RCC) matches said device region code (RCD), as taught in element 6 above.

Kocher teaches at col. 7, lines 55-60 a CryptoFirewall, which is a specialized circuit placed between the interface control processor (ICP) and a protected memory to control access to the protected memory, even if the ICP is compromised. The CryptoFirewall uses the protected memory to **derive decryption keys.** It is submitted deriving a decryption key is different from teaching decrypting said region key (RK) using said device key (DK) in case said carrier region code (RCC) matches said device region code (RCD), as taught in element 6 above.

Kocher at col. 8, lines 18-28 teaches a Key Derivation Message (KDM), which is a message generated by a content provider to allow a CRU to **derive a decryption key** corresponding to some digital content. It is submitted deriving a decryption key is different from teaching decrypting said region key (RK) using said device key (DK) in case said carrier region code (RCC) matches said device region code (RCD), as taught in element 6 above.

The Examiner refers the Applicant to Kocher at col. 8, lines 52-55 which teaches a Rights Key, such as a cryptographic key, that allows a CRU to generate or decode the decryption keys for some content. It is submitted generating and/or decoding decryption keys is different from teaching decrypting said region key (RK) using said device key (DK) in case said carrier region code (RCC) matches said device region code (RCD), as taught in element 6 above.

Based at least on the arguments presented above, it is respectfully submitted that Kocher does not disclose or suggest element 6 above as alleged in the outstanding Office Action.

Element 8 Not Disclosed by Kocher

It respectfully submitted that Kocher does not disclose or suggest a reproducing apparatus comprising **a content decryption means for decrypting said encrypted content using said decrypted region key** and output means for outputting said decrypted content, as recited in element 8 above.

The Examiner asserts that element 8 is allegedly taught in Kocher at col. 4, lines 14-34, col. 7, lines 55-60, col. 8, lines 18-28 & 52-55, col. 9, lines 37-59 and at col. 11, lines 33-65. Applicant respectfully disagrees.

The Examiner refers the Applicant to Kocher at col. 4, lines 14-24 which teaches that software stored in a ROM or EEPROM **manages protocols and cryptographic keys** involved in decrypting content. This process may be assisted by a cryptographic processor. The cryptographic keys taught at col. 4, lines 33-35 are keys associated with either pre-payment or post-payment and not content decryption means for decrypting said encrypted content using said decrypted region key, as taught in element 8 above.

The Examiner also refers the Applicant to Kocher at col. 7, lines 55-60 which teaches that software stored in a ROM or EEPROM **manages protocols and cryptographic keys** involved in decrypting content. This process may be assisted by a cryptographic processor. The cryptographic keys taught at col. 4, lines 33-35 are keys associated with either pre-payment or post-payment and not content decryption means for

decrypting said encrypted content using said decrypted region key, as taught in element 8 above.

The Examiner also refers the Applicant to Kocher at col. 7, lines 55-60, which teaches a CryptoFirewall, which is a specialized circuit placed between the interface control processor (ICP) and a protected memory to control access to the protected memory, even if the ICP is compromised. The CryptoFirewall uses the protected memory to **derive decryption keys.** It is submitted that Kocher only teaches the derivation of decryption keys and not content decryption means for decrypting said encrypted content using said decrypted region key, as taught in element 8 above.

The Examiner also refers the Applicant to Kocher at col. 8, lines 18-28 which teaches a Key Derivation Message (KDM), which is a message generated by a content provider to allow a CRU to **derive a decryption key** corresponding to some digital content. It is submitted that Kocher only teaches the derivation of decryption keys and not content decryption means for decrypting said encrypted content using said decrypted region key, as taught in element 8 above.

The Examiner also refers the Applicant to Kocher at col. 8, lines 52-55 which teaches a Rights Key, such as a cryptographic key, that allows a CRU to generate or decode the decryption keys for some content. It is submitted that Kocher only teaches the generation or decoding of decryption keys and not **content decryption means for decrypting said encrypted content using said decrypted region key,** as taught in element 8 above.

Based on at least the arguments presented above, it is respectfully submitted that Kocher does not disclose or suggest element 8 above as alleged in the outstanding Office Action.

35 U.S.C. §103(a)

Claim 4-8 was rejected under 35 U.S.C. §103(a) as being unpatentable over Kocher and Bednarak as applied to claim 1 above and further in view of U.S. Patent No. 5,907,655 to Oguro.
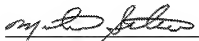
Claims 4-8 depend from Claim 1 and therefore include the limitations of Claim 1. Accordingly, for the same reasons given above for Claim 1, Claims 4-8 are believed to contain patentable subject matter. Accordingly, withdrawal of the rejections with respect to Claims 4-8 and allowance thereof are respectfully requested.

Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that all claims presently pending in the application, namely, Claims 1- 13 are believed to be in condition for allowance and patentably distinguishable over the art of record.

If the Examiner should have any questions concerning this communication or feels that an interview would be helpful, the Examiner is requested to call Mike Belk, Esq., Intellectual Property Counsel, Philips Electronics North America, at 914-945-6000.

Respectfully submitted,

Michael A. Scaturro
Reg. No. 51,356
Attorney for Applicant

Mailing Address:
Intellectual Property Counsel
Philips Electronics North America Corp.
P.O. Box 3001
345 Scarborough Road
Briarcliff Manor, New York 10510-8001